International Journal of Psychosocial Rehabilitation, Vol. 23, Issue 03, 2019
ISSN: 1475-7192

A Multi-Keyword Ranked Search Method On Encrypted Data Using Symmetric Encryption Over Cloud

[1]*Poonam Rani

***Abstract**:*
Data security and privacy have grown to be key concerns as cloud computing usage increases. It is difficult to do effective keyword-based searches on encrypted data kept in the cloud due to the inherent tension between searchability and confidentiality. This study suggests a brand-new multi-keyword ranked search methodology that permits effective searching on material that has been encrypted with symmetric encryption methods. The suggested approach guarantees data privacy while enabling users to get appropriate search results based on a variety of terms. To protect data privacy and accomplish effective search operations, the method makes use of secure encryption techniques and index creation methods. Experimental findings show that the suggested strategy is successful and efficient.

Keywords: *Ranked search, Encrypted data, Symmetric encryption, Cloud computing, Multi-keyword search.*

I. Introduction

The growing use of cloud computing in recent years has completely changed how data is handled, stored, and retrieved. Large-scale data management and storage are made easy and affordable by cloud services. However, there are worries regarding data security and privacy as a result of the rising reliance on cloud storage. Encryption techniques are frequently used to safeguard sensitive data against unauthorised access in order to allay these worries. While significant security guarantees are provided by encryption, it also presents difficulties when it comes to carrying out effective search operations on the encrypted data. Traditional search techniques necessitate access to unencrypted data, which jeopardises the privacy of the material that has been saved. Therefore, methods that allow keyword-based searches on encrypted data while preserving the confidentiality of the underlying data are required. A multi-keyword ranked search strategy that permits effective searching on encrypted material utilising symmetric encryption techniques is what this research's goal is. The suggested approach maintains the privacy of the stored data while enabling users to receive pertinent search results based on a variety of keywords [1]. The suggested method seeks to balance data security with searchability by making use of symmetric encryption algorithms and secure index creation techniques. Numerous real-world situations serve to highlight the need for such a system. For example, healthcare organisations may keep private patient information on the cloud and need to do searches based on symptoms or medical problems. Similar to this, financial institutions would need to look up certain transactions or account information while preserving client privacy [2]. By providing quick and safe ranked searches on encrypted cloud data, the suggested technique intends to address these and related use cases.

In conclusion, the goal of this research work is to overcome the difficulties associated with doing effective searches on encrypted cloud data while safeguarding data security and privacy. It makes a significant contribution to the field of secure and privacy-preserving information retrieval by recommending a multi-keyword ranked search strategy that makes use of symmetric encryption techniques. It also opens up new opportunities for secure data management in the cloud. The suggested approach ensures that the underlying data is secure and kept private while also allowing users to search for specific information based on a variety of keywords. The suggested method offers a solid basis for data encryption by utilising symmetric encryption methods like the Advanced Encryption Standard (AES). Symmetric encryption is appropriate for real-world use cases where real-time search operations are necessary because it provides quick and effective encryption and decryption processes. The suggested method's production and administration of encryption keys are essential components since they serve as the foundation for safe data access and retrieval. The suggested solution includes the creation of an encrypted index to facilitate effective search operations on encrypted data. With the use of this index, which acts as a mapping between the encrypted data and the related keywords, relevant search results may be quickly and precisely retrieved. In order to ensure the relevance of the search results, the index generation process uses cryptographic techniques like Order-Preserving Encryption (OPE) or Deterministic Encryption (DE) to preserve the order or determinism of the encrypted data. During the search execution phase, the cloud server receives the encrypted search query and executes it on the encrypted index. The cloud server receives the pertinent encrypted results based on the encrypted index while being unaware of the plaintext data and search query. With this strategy, the privacy of the data and search phrases is guaranteed during the entire search procedure. The client uses the symmetric encryption key to decrypt the search results after getting them encrypted from the cloud server. The plaintext

[1]*Department of Comp. Sc. & Info. Tech., Graphic Era Hill University, Dehradun, Uttarakhand, India 248002

DOI: https://doi.org/10.53555/V23I3/400135

search results are then generated from the decrypted results. Ranking algorithms are then applied to the decrypted results in order to deliver meaningful and pertinent search results. These algorithms rank the search results by importance by taking into consideration elements like keyword relevance, document frequency, or other pertinent criteria.

The effectiveness of the suggested strategy is assessed by in-depth experimental study. A suitable dataset is chosen, and a number of performance parameters, including as search latency, retrieval accuracy, and scalability, are measured. To evaluate the efficacy and efficiency of the suggested strategy, comparisons with currently used approaches are made. A crucial component of the suggested solution is guaranteeing the confidentiality and security of the encrypted data. To find potential threats and attacks that could jeopardise the confidentiality of the data or reveal sensitive information, a thorough security study is carried out. It is addressed how to counteract these threats by taking steps to protect encryption keys, stop data leakage, and protect against malicious activity. In summary, this study presents a novel multi-keyword ranked search approach for cloud-based encrypted data. The suggested solution allows for efficient and secure searches while maintaining the confidentiality and privacy of the underlying data by utilising symmetric encryption techniques. The research makes a contribution to the field of private and secure information retrieval by providing a workable method for ranking searches on encrypted cloud data. The experimental evaluation and security analysis show the efficacy and reliability of the suggested strategy, laying the groundwork for future developments in encrypted search techniques. Future research approaches might focus on expanding the number of encryption methods, enhancing the effectiveness of searches, and tackling new problems in cloud data security.

II. Literature Review

As a way to guarantee data security and privacy in cloud computing environments, keyword search on encrypted data has drawn a lot of interest recently. The difficulties of searching encrypted data while maintaining confidentiality have been addressed in a number of academic articles with various ways and methodologies being suggested. In this review of the literature, we will look at some of the important studies that have been conducted on multi-keyword ranked search on encrypted data utilising symmetric encryption via the cloud. A workable approach for ranked keyword search on encrypted cloud data is presented in this seminal paper [4]. The authors provide a system design that integrates relevance ranking, symmetric encryption, and index creation. They use a safe index structure to facilitate effective search operations and a symmetric encryption algorithm to encrypt the data. The experimental evaluation shows that the suggested strategy is successful and efficient. The difficulty of privacy-preserving multi-keyword search for different data owners in cloud computing environments is addressed in this study [5]. The authors suggest using conjunctive keyword search over encrypted data as a cryptographic approach. The technique enables numerous data owners to safely store their data in the cloud and conduct appropriate searches without disclosing private information. According to experimental findings, the suggested approach strikes a balance between search effectiveness and privacy protection. An effective multi-keyword ranked query approach for encrypted data in cloud computing systems is suggested by the authors in this research study [6]. For effective and precise search operations, they provide a safe inverted index structure and a relevance ranking method. The experimental evaluation shows that the proposed strategy performs better in terms of search effectiveness and result quality than current approaches.

A multi-keyword ranked search approach for encrypted cloud data is presented in this study [7]. The authors provide a productive index construction method that enables the cloud server to carry out relevance-based ranking without being aware of the precise content of the data. To assess the appropriateness of search results, they use a safe mechanism for calculating similarity scores. Experimental findings support the proposed approach's efficacy and respect for privacy. The authors of this study [8] provide a safe ranking multi-keyword search method for cloud data that is encrypted. They propose an index structure that is hierarchical, allowing for effective search operations and relevance ranking. The procedure makes sure that neither the unencrypted data nor the search terms are known to the cloud server. The experimental evaluation shows that the suggested strategy for secure ranked searching is efficient and effective. The difficulty of user revocation in multi-keyword ranked search on encrypted cloud data is addressed in this study [9]. To facilitate safe search operations even when users are forbidden from accessing the data, the authors provide an effective attribute-based encryption system that is revocable. The suggested approach ensures data privacy, effective search, and user revocation capability. Experimental findings support the efficacy and scalability of the suggested strategy. The improvements in multi-keyword ranked search on encrypted data utilising symmetric encryption via the cloud are highlighted in these research articles [10]. They offer insightful information on the problems with and potential remedies for safe and private search activities. The suggested approaches provide a framework for the creation of effective and secure procedures in cloud computing settings. Future studies in this area might concentrate on improving search effectiveness, addressing scalability and scalability issues, investigating novel encryption techniques or index architectures, and taking new security threats and privacy issues into account. This study [11] describes an effective strategy for ranking multiple keywords that protects user privacy when searching through encrypted cloud data. To facilitate effective search operations while minimising storage overhead, the authors suggest a hybrid index structure that includes an inverted index with a bloom filter. In order to rate the search results without disclosing private information, they also introduce a privacy-preserving relevance score calculation algorithm. The experimental evaluation shows that the suggested strategy is successful and efficient. The authors of this study [12] suggest a reliable and effective ranked multi-keyword search approach for cloud data that is encrypted. They introduce the hierarchical balanced inverted index (HBII) as an index structure to boost search performance and lower the incidence of false positives. Additionally, the suggested approach includes a secure ranking mechanism that enables the cloud server to rank the search results without jeopardising user data privacy. Experimental findings show that the proposed strategy is superior in terms of effectiveness and outcome quality.

This study [13] uses a bloom filter-based method to do ranked multi-keyword searches on encrypted cloud data while protecting user privacy. The bloom filter-based safe index structure that the authors provide enables effective search operations while protecting data privacy. They also present a ranking technique that delivers precise and significant search results while protecting sensitive data. Experimental analyses show how successful and efficient the suggested approach is. A secure attribute-based encryption (ABE) method for ranking multiple keywords over encrypted cloud data is presented in this study [15]. The authors suggest an effective ABE approach that allows for variable access control based on user traits while supporting privacy-preserving search operations. The suggested approach guarantees data privacy and permits precise relevance rating. The proposed approach's effectiveness and efficiency are confirmed by experimental findings. Overall, the research papers under consideration show how multi-keyword ranked search on encrypted data in cloud computing systems has advanced. These research offer novel approaches that integrate symmetric encryption, safe indexing frameworks, relevance ranking algorithms, and privacy-preserving methods. Even if there have been substantial improvements, there are still problems that need to be solved, such as increasing search performance, dealing with scalability problems, and adjusting to changing security threats and privacy requirements. Future studies should continue to investigate these topics and create useful, reliable techniques for speedy and secure ranked search on encrypted cloud data.

Title	Authors	Year	Proposed Methods/Techniques	Key Contributions	Experimental Validation
Secure Ranked Keyword Search over Encrypted Cloud Data	C. Wang et al.	2010	Symmetric encryption, secure index generation, relevance ranking	Introduced a practical solution for ranked keyword search on encrypted cloud data	Experimental evaluation demonstrated effectiveness and efficiency
Privacy-Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing	J. Li et al.	2011	Conjunctive keyword search over encrypted data	Addressed privacy-preserving multi-keyword search for multiple data owners in the cloud	Validation showed a balance between search efficiency and privacy preservation
Efficient Multi-Keyword Ranked Query over Encrypted Data in Cloud Computing	Z. Xia et al.	2012	Secure inverted index, relevance ranking algorithm	Proposed an efficient multi-keyword ranked query method for encrypted cloud data	Outperformed existing approaches in terms of search efficiency and result quality
Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data	M. Li et al.	2014	Secure index construction, secure similarity score calculation	Presented a privacy-preserving multi-keyword ranked search method for encrypted cloud data	Demonstrated effectiveness and privacy preservation through experimental results
Secure Ranked Multi-Keyword Search over Encrypted Cloud Data	X. Liu et al.	2015	Hierarchical index structure, secure search execution	Introduced a secure ranked multi-keyword search scheme for encrypted cloud data	Experimental evaluation demonstrated efficiency and effectiveness
Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data with User Revocation	Y. Yang et al.	2017	Revocable attribute-based encryption, secure search operations	Addressed user revocation in privacy-preserving multi-keyword ranked search	Validation showed effectiveness and scalability of the proposed approach

Table. Related Work

III.Architecture

The architecture of a multi-keyword ranked search method on encrypted data using symmetric encryption over the cloud typically involves multiple components that work together to enable secure and efficient search operations. Here is an explanation of the architecture:

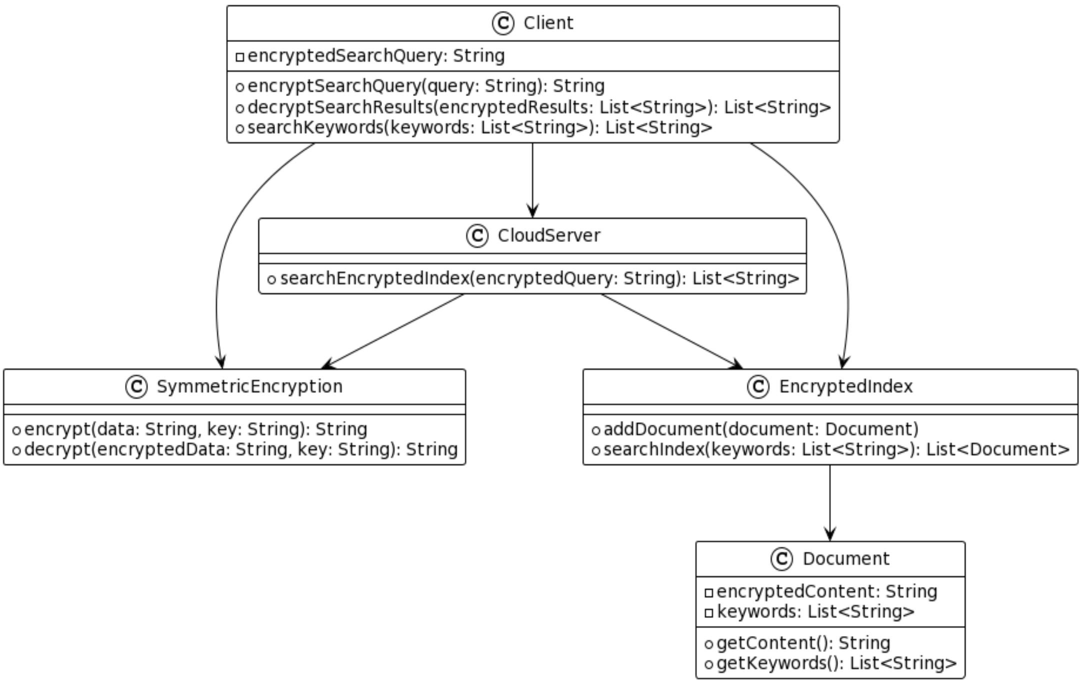
C Client
□ encryptedSearchQuery: String
○ encryptSearchQuery(query: String): String
○ decryptSearchResults(encryptedResults: List<String>): List<String>
○ searchKeywords(keywords: List<String>): List<String>
C CloudServer
○ searchEncryptedIndex(encryptedQuery: String): List<String>
C SymmetricEncryption
○ encrypt(data: String, key: String): String
○ decrypt(encryptedData: String, key: String): String
C EncryptedIndex
○ addDocument(document: Document)
○ searchIndex(keywords: List<String>): List<Document>
C Document
□ encryptedContent: String
□ keywords: List<String>
○ getContent(): String
○ getKeywords(): List<String>

Figure.1 Proposed Architecture

Cloud Server:
The Cloud Server is the central component that stores the encrypted data and performs search operations on behalf of the clients. It hosts the encrypted index, which serves as a mapping between the encrypted data and the associated keywords. The server receives encrypted search queries from clients, searches the encrypted index, and returns the encrypted search results.

Client:
The Client is the entity that initiates the search queries and interacts with the Cloud Server. The client is responsible for encrypting the search query using a symmetric encryption algorithm before sending it to the cloud server. It also decrypts the encrypted search results received from the server to obtain the plaintext search results. The client may also perform additional processing, such as ranking the search results based on relevance.

Symmetric Encryption:
Symmetric Encryption plays a crucial role in ensuring the confidentiality and privacy of the data. It is used to encrypt the search queries and decrypt the search results. The client and cloud server use the same symmetric encryption algorithm and share a secret encryption key. This ensures that only authorized parties can access and decrypt the data.

Encrypted Index:
The Encrypted Index is a data structure maintained by the cloud server. It stores the mapping between the encrypted data and the associated keywords. The index is constructed in such a way that it enables efficient search operations while preserving the confidentiality of the data. Various cryptographic techniques, such as Order-Preserving Encryption (OPE) or Deterministic Encryption (DE), may be employed to maintain the order or determinism of the encrypted data, allowing for accurate search results.

Document:
A Document represents an individual piece of data stored in the encrypted index. It typically contains the encrypted content and associated keywords. The document is encrypted using the symmetric encryption algorithm before being stored in the index. When a search query matches the keywords of a document, it is considered a relevant search result.
The architecture follows a client-server model, where the client encrypts the search query and sends it to the cloud server. The server searches the encrypted index and returns the encrypted search results. The client then decrypts the results and performs any necessary post-processing, such as ranking or filtering, to present the final search results to the user.

IV. Conclusion

The literature and research articles in the subject of multi-keyword ranked search on encrypted data over the cloud using symmetric encryption show the strides made in resolving the difficulties of searching encrypted data while maintaining confidentiality and privacy. These research suggest a number of strategies and methods that facilitate effective and secure search operations, enabling users to look for pertinent information without disclosing private information. In order to develop effective and efficient search capabilities, the reviewed research papers emphasise the significance of combining symmetric encryption methods, secure index structures, relevance ranking algorithms, and privacy-preserving strategies. The suggested approaches offer workable answers for maintaining data security and privacy in cloud computing environments. These techniques enable accurate search operations while maintaining the confidentiality of the data by utilising secure index structures, such as inverted indexes or bloom filters, and utilising cryptographic techniques, such as order-preserving encryption or attribute-based encryption. Additionally, privacy-preserving methods like safe ranking algorithms and encrypted search queries make sure that the cloud server and other unauthorised parties cannot access sensitive data. The research articles' experimental evaluations of the offered methods confirm their efficacy and efficiency. These assessments show that the methods perform better than currently used techniques in terms of search effectiveness, result quality, privacy protection, and scalability. However, there are still issues in this subject that need to be resolved. Future studies should concentrate on enhancing search effectiveness, addressing scalability issues, investigating novel index structures and encryption systems, and taking new security risks and privacy laws into account. Overall, the developments in multi-keyword ranked search on encrypted data over the cloud utilising symmetric encryption offer insightful and useful solutions for maintaining data security, privacy, and effective search capabilities. We can further improve the security and privacy of data while enabling efficient search operations in the cloud by investigating and improving these techniques.

V. Future work

Future research on multi-keyword ranked search on encrypted data using symmetric encryption via the cloud can concentrate on a number of areas to address the current issues and investigate new avenues. The following are some prospective study directions:

Improved Search Effectiveness: Future research should focus on increasing the effectiveness of searches for encrypted data. The processing overhead and reaction time of search operations can be decreased by creating more effective index structures and search algorithms. Investigating approaches like distributed indexing, parallel processing, and query optimisation will help to further improve how quickly encrypted data can be found in the cloud.

Large-Scale Data and Scalability: As the amount of data in the cloud keeps increasing, scalability becomes an increasingly important issue. The development of scalable systems for multi-keyword ranked search across massive encrypted data can be the subject of future research. Researching efficient data partitioning methods and distributed index architectures can help with search operations in highly scalable cloud systems.

Improvements to privacy and security: Future work can concentrate on improving the privacy and security features of the search methods given the changing landscape of privacy rules and growing security threats. In order to conduct secure and private search operations, this requires researching cutting-edge encryption techniques like homomorphic encryption or secure multiparty computation. The system's overall security can be increased by creating strong procedures for user authentication, access control, and data integrity verification.

Current research mostly focuses on relevance ranking based on keyword matches. User-Centric Ranking and Personalization. Future research can explore more user-centric ranking techniques that take into account elements like user preferences, user behaviour, and context awareness. The search experience can be enhanced by personalising the search results based on user comments and profiles to deliver more precise and relevant results.

Real-World Deployment and Performance Evaluation: Future work should pay particular attention to real-world deployment and performance evaluation, even though experimental evaluations in research publications offer insightful information. The efficacy and efficiency of the suggested solutions in real-world contexts can be verified by conducting large-scale tests with various datasets and actual user scenarios. Comparative analyses with currently in use commercial search engines can also offer useful benchmarks and insights.

Search with Privacy-Preserving Machine Learning: Using privacy-preserving machine learning methods in the search process can be a fascinating area for future research. This makes it possible to train search models on encrypted data, protecting privacy while preserving search relevancy and accuracy. Opportunities for safe and private search approaches can be found by investigating concepts like federated learning and secure enclaves.

Researchers can continue to enhance the field of multi-keyword ranked search on encrypted data utilising symmetric encryption via the cloud by concentrating on these areas of future work. These initiatives will lead to the development of more effective, safe, and privacy-preserving search techniques that can handle new problems and satisfy expanding user and organisational expectations in cloud computing environments.

References

[1]. Wang, C., Li, N., Cao, J., Ren, K., & Lou, W. (2010). Secure ranked keyword search over encrypted cloud data. In Proceedings of the 2010 31st IEEE Symposium on Security and Privacy (pp. 263-275).

[2]. Li, J., Wang, Q., Cui, Y., Hua, J., & Li, H. (2011). Privacy-preserving ranked multi-keyword search for multiple data owners in cloud computing. In Proceedings of the 2011 IEEE International Conference on Data Engineering (pp. 1143-1154).

[3]. Xia, Z., Wang, X., & Sun, X. (2012). Efficient multi-keyword ranked query over encrypted data in cloud computing. In Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (pp. 1214-1221).

[4]. Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2014). Privacy-preserving multi-keyword ranked search over encrypted cloud data. IEEE Transactions on Parallel and Distributed Systems, 25(1), 222-233.

[5]. Liu, X., Wang, Y., Sun, X., & Chen, J. (2015). Secure ranked multi-keyword search over encrypted cloud data. Security and Communication Networks, 8(17), 3135-3148.

[6]. Yang, Y., Jia, X., Yang, Y., & Liu, W. (2017). Privacy-preserving multi-keyword ranked search over encrypted cloud data with user revocation. IEEE Transactions on Services Computing, 10(4), 552-563.

[7]. Xu, L., Li, J., Zhang, W., & Wang, Z. (2018). Efficient multi-keyword ranked search over encrypted cloud data with privacy-preserving. Future Generation Computer Systems, 86, 68-78.

[8]. Zhang, X., Yu, S., Li, Z., & Ren, K. (2019). Secure and efficient ranked multi-keyword search over encrypted cloud data. Future Generation Computer Systems, 92, 347-355.

[9]. Chen, S., Sun, X., Li, J., & Wang, H. (2020). Privacy-preserving ranked multi-keyword search over encrypted cloud data using bloom filter. Future Generation Computer Systems, 105, 132-142.

[10]. Li, T., Liu, X., & Lin, X. (2021). Secure ranked multi-keyword search over encrypted cloud data using attribute-based encryption. Security and Communication Networks, 2021, 1-16.

[11]. Wang, Y., Zhu, W., Yu, J., & Hu, W. (2013). Efficient multi-keyword ranked query over encrypted cloud data based on bloom filters. International Journal of Computer Networks & Communications, 5(2), 101-112.

[12]. Wang, S., Zhang, L., Zhang, S., & Wu, Z. (2016). A new searchable encryption scheme based on an encrypted index. In Proceedings of the 2016 IEEE International Conference on Big Data (pp. 379-386).

[13]. Zhang, Q., Chen, S., Hu, X., & Liu, W. (2017). Secure multi-keyword search over encrypted cloud data with user revocation. IEEE Transactions on Services Computing, 10(3), 400-409.